Refine Search

Search Results -

Terms	Documents
L7 AND hash	0

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L8

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Friday, March 11, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=TDBD; PLUR=NO; OP=OR			
L8	L7 AND hash	0	L8
L7	smartcard OR javaCARd Or (java ADJ card)	7	L7
DB=USPT; PLUR=NO; OP=OR			
L6	L5 AND hash	13	L6
L5	L4 AND (optimization or optimisation)	42	L5
L4	smartcard OR javaCARd Or (java ADJ card)	834	L4
DB=PGPB; PLUR=NO; OP=OR			
L3	L2 AND hash	26	L3
L2	L1 AND optimization	51	L2
L1	smartcard OR javaCARd Or (java ADJ card)	1078	L1

END OF SEARCH HISTORY

Refine Search

Search Results -

Terms	Documents
L1 AND optimization	51

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L2

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Friday, March 11, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB; PLUR=NO; OP=OR			
L2	L1 AND optimization	51	L2
L1	smartcard OR javaCARd Or (java ADJ card)	1078	L1

END OF SEARCH HISTORY

Refine Search

Search Results -

Terms	Documents
L5 AND hash	13

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L6

Refine Search

Recall Text | Clear | Interrupt

Search History

DATE: Friday, March 11, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=NO; OP=OR			
L6	L5 AND hash	13	L6
L5	L4 AND (optimization or optimisation)	42	L5
L4	smartcard OR javaCARd Or (java ADJ card)	834	L4
DB=PGPB; PLUR=NO; OP=OR			
L3	L2 AND hash	26	L3
L2	L1 AND optimization	51	L2
L1	smartcard OR javaCARd Or (java ADJ card)	1078	L1

END OF SEARCH HISTORY

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 13 of 13 returned.

☑ 1. Document ID: US 6859533 B1

L6: Entry 1 of 13 File: USPT Feb 22, 2005

US-PAT-NO: 6859533
DOCUMENT-IDENTIFIER: US 6859533 B1

TITLE: System and method for transferring the right to decode messages in a symmetric encoding scheme

DATE-ISSUED: February 22, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Wang; Xin	Los Angeles	CA		
Ta; Thanh T.	Huntington Beach	CA		

US-CL-CURRENT: 380/28; 380/259

ABSTRACT:

Methods for transferring among key holders in encoding and cryptographic systems the right to decode and decrypt messages in a way that does not explicitly reveal decoding and decrypting keys used and the original messages. Such methods are more secure and more efficient than typical re-encoding and re-encryption schemes, and are useful in developing such applications as document distribution and long-term file protection.

11 Claims, 14 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 14

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 2. Document ID: US 6850909 B1

L6: Entry 2 of 13 File: USPT Feb 1, 2005

US-PAT-NO: 6850909
DOCUMENT-IDENTIFIER: US 6850909 B1

TITLE: Using smartcards to enable probabilistic transactions on an untrusted device

DATE-ISSUED: February 1, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Aiello; William A.	Madison	NJ		
Rubin; Aviel D.	West Caldwell	NJ		
Strauss; Martin J.	Summit	NJ		

US-CL-CURRENT: 705/50; 380/228, 380/239, 380/272, 713/162, 713/171, 713/200

ABSTRACT:

The present invention permits a user to conduct remote transactions without a network while using an untrusted computing device, such as a hand-held personal digital assistant or a laptop computer. The computing device is augmented with a smartcard reader, and the user obtains a smartcard and connects it to the device. This design can be used by an untrusted user to perform financial transactions, such as placing bets on the outcome of a probabilistic computation. Protocols are presented for adding (purchasing) or removing (selling) value on the smartcard, again without requiring a network connection. Using the instant protocols, neither the user nor the entity issuing the smartcards can benefit from cheating.

8 Claims, 6 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 5

☐ 3. Document ID: US 6850252 B1

L6: Entry 3 of 13 File: USPT Feb 1, 2005

US-PAT-NO: 6850252
DOCUMENT-IDENTIFIER: US 6850252 B1

TITLE: Intelligent electronic appliance system and method

DATE-ISSUED: February 1, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Hoffberg; Steven M.	West Harrison	NY	10994	

US-CL-CURRENT: 715/716; 380/252, 715/719, 715/727

ABSTRACT:

An intelligent electronic appliance preferably includes a user interface, data input and/or output port, and an intelligent processor. A preferred embodiment comprises a set top box for interacting with broadband media streams, with an adaptive user interface, content-based media processing and/or media metadata processing, and telecommunications integration. An adaptive user interface models

the user, by observation, feedback, and/or explicit input, and presents a user interface and/or executes functions based on the user model. A content-based media processing system analyzes media content, for example audio and video, to understand the content, for example to generate content-descriptive metadata. A media metadata processing system operates on locally or remotely generated metadata to process the media in accordance with the metadata, which may be, for example, an electronic program guide, MPEG 7 data, and/or automatically generated format. A set top box preferably includes digital trick play effects, and incorporated digital rights management features.

22 Claims, 32 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 28

☐ 4. Document ID: US 6786420 B1

L6: Entry 4 of 13 File: USPT Sep 7, 2004

US-PAT-NO: 6786420
DOCUMENT-IDENTIFIER: US 6786420 B1

TITLE: Data distribution mechanism in the form of ink dots on cards

DATE-ISSUED: September 7, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Silverbrook; Kia	Sydney			AU

US-CL-CURRENT: 235/494

ABSTRACT:

An improved form of information distribution information distribution medium is disclosed comprising a card on which at least one surface thereof contains distributed information encoded as an array of dots printed on the surface in a fault tolerant manner. Preferably, the array of dots is grouped into a plurality of data segment blocks with each data segment block having a delineated border region for accurately spatially locating the dots. The delineated border region can include a series of periodically spaced markers, the periodicity being substantially twice the pitch of the array of dots. The delineated border region can further include at least one line of dots spaced adjacent to the periodically spaced markers. The periodically spaced markers can comprise substantially 2 or 3 adjacent printed dots. Applications and uses of such-a system are also disclosed.

8 Claims, 232 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 140

☐ 5. Document ID: US 6772331 B1

L6: Entry 5 of 13 File: USPT Aug 3, 2004

US-PAT-NO: 6772331
DOCUMENT-IDENTIFIER: US 6772331 B1

TITLE: Method and apparatus for exclusively pairing wireless devices

DATE-ISSUED: August 3, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Hind; John Raithel	Raleigh	NC		
Peters; Marcia Lambert	Raleigh	NC		

US-CL-CURRENT: 713/151; 370/313, 707/10, 707/9, 713/178, 713/182, 713/200

ABSTRACT:

A method and system for enabling wireless devices to be paired or permanently associated by a user or a network administrator. The method and system utilize well known public key cryptography and machine unique identifiers to establish a secure channel and associate the devices with eachother. This is extremely useful for associating a wireless headset with a telephone or associating a wireless mouse with a computer.

45 Claims, 9 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 9

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. D

☐ 6. Document ID: US 6609199 B1

L6: Entry 6 of 13 File: USPT Aug 19, 2003

US-PAT-NO: 6609199
DOCUMENT-IDENTIFIER: US 6609199 B1

TITLE: Method and apparatus for authenticating an open system application to a portable IC device

DATE-ISSUED: August 19, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
DeTreville; John	Seattle	WA		

US-CL-CURRENT: 713/172; 713/156, 713/157, 713/168, 713/169, 713/175

ABSTRACT:

A secure communication channel between an open system and a portable IC device is established. An application running on the open system desiring access to the information on the portable IC device authenticates itself to the portable IC device, proving that it is trustworthy. Once such trustworthiness is proven, the portable IC device authenticates itself to the application. Once such two-way authentication has been completed, trusted communication between the open system and the portable IC device can proceed, and private information that is maintained on the portable IC device can be unlocked and made available to the application.

30 Claims, 15 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 13

☐ 7. Document ID: US 6496808 B1

L6: Entry 7 of 13 File: USPT Dec 17, 2002

US-PAT-NO: 6496808
DOCUMENT-IDENTIFIER: US 6496808 B1
**** See image for Certificate of Correction ****

TITLE: Using smartcards to enable probabilistic transaction on an untrusted device

DATE-ISSUED: December 17, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Aiello; William A.	Madison	NJ		
Rubin; Aviel D.	West Caldwell	NJ		
Strauss; Martin J.	Summit	NJ		

US-CL-CURRENT: 705/67; 380/228, 713/200

ABSTRACT:

The present method permits a user to conduct remote transactions without a network while using an untrusted computing device, such as a hand-held personal digital assistant or a laptop computer. The computing device is augmented with a smartcard reader, and the user obtains a smartcard and connects it to the device. This design can be used by an untrusted user to perform financial transactions, such as placing bets on the outcome of a probabilistic computation. Protocols are presented for adding (purchasing) or removing (selling) value on the smartcard, again without requiring a network connection. Using the instant protocols, neither the user nor the entity issuing the smartcards can benefit from cheating.

4 Claims, 6 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 5

☐ 8. Document ID: US 6381699 B2

L6: Entry 8 of 13 File: USPT Apr 30, 2002

US-PAT-NO: 6381699
DOCUMENT-IDENTIFIER: US 6381699 B2

TITLE: Leak-resistant cryptographic method and apparatus

DATE-ISSUED: April 30, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kocher; Paul C.	San Francisco	CA		
Jaffe; Joshua M.	San Francisco	CA		

US-CL-CURRENT: 713/172; 705/65, 713/174, 713/340

ABSTRACT:

The present invention provides a method and apparatus for securing cryptographic devices against attacks involving external monitoring and analysis. A "self-healing" property is introduced, enabling security to be continually re-established following partial compromises. In addition to producing useful cryptographic results, a typical leak-resistant cryptographic operation modifies or updates secret key material in a manner designed to render useless any information about the secrets that may have previously leaked from the system. Exemplary leak-proof and leak-resistant implementations of the invention are shown for symmetric authentication, certified Diffie-Hellman (when either one or both users have certificates), RSA, ElGamal public key decryption, ElGamal digital signing, and the Digital Signature Algorithm.

18 Claims, 4 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 4

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. De

☑ 9. Document ID: US 6314409 B1

L6: Entry 9 of 13 File: USPT Nov 6, 2001

US-PAT-NO: 6314409
DOCUMENT-IDENTIFIER: US 6314409 B1

TITLE: System for controlling access and distribution of digital property

DATE-ISSUED: November 6, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Schneck; Paul B.	Potomac	MD		
Abrams; Marshall D.	Silver Spring	MD		

US-CL-CURRENT: 705/54; 380/259, 380/287, 380/59, 705/57, 713/182, 713/189, 713/193, 713/194, 713/200

ABSTRACT:

A method and device are provided for controlling access to data. Portions of the data are protected and rules concerning access rights to the data are determined. Access to the protected portions of the data is prevented, other than in a non-useable form; and users are provided access to the data only in accordance with the rules as enforced by a mechanism protected by tamper detection. A method is also provided for distributing data for subsequent controlled use of those data. The method includes protecting portions of the data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing a package including: the protected portions of the data and the protected rules. A user is provided controlled access to the distributed data only in accordance with the rules as enforced by a mechanism protected by tamper protection. A device is provided for controlling access to data having protected data portions and rules concerning access rights to the data. The device includes means for storing the rules; and means for accessing the protected data portions only in accordance with the rules, whereby user access to the protected data portions is permitted only if the rules indicate that the user is allowed to access the portions of the data.

43 Claims, 34 Drawing figures
Exemplary Claim Number: 35
Number of Drawing Sheets: 26

☐ 10. Document ID: US 6304658 B1

L6: Entry 10 of 13 File: USPT Oct 16, 2001

US-PAT-NO: 6304658
DOCUMENT-IDENTIFIER: US 6304658 B1
**** See image for Certificate of Correction ****

TITLE: Leak-resistant cryptographic method and apparatus

DATE-ISSUED: October 16, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kocher; Paul C.	San Francisco	CA		
Jaffe; Joshua M.	San Francisco	CA		

US-CL-CURRENT: 380/30; 380/28, 380/44

ABSTRACT:

The present invention provides a method and apparatus for securing cryptographic devices against attacks involving external monitoring and analysis. A "self-healing" property is introduced, enabling security to be continually re-established following partial compromises. In addition to producing useful cryptographic results, a typical leak-resistant cryptographic operation modifies or updates secret key material in a manner designed to render useless any information about the secrets that may have previously leaked from the system. Exemplary leak-proof and leak-resistant implementations of the invention are shown for symmetric authentication, certified Diffie-Hellman (when either one or both users have certificates), RSA, ElGamal public key decryption, ElGamal digital signing, and the Digital Signature Algorithm.

54 Claims, 4 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 4

☐ 11. Document ID: US 6192472 B1

L6: Entry 11 of 13 File: USPT Feb 20, 2001

US-PAT-NO: 6192472
DOCUMENT-IDENTIFIER: US 6192472 B1

TITLE: Method and apparatus for the secure distributed storage and retrieval of information

DATE-ISSUED: February 20, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Garay; Juan Alberto	Yonkers	NY		
Gennaro; Rosario	New York	NY		
Jutla; Charanjit Singh	Elmsford	NY		
Rabin; Tal D.	Riverdale	NY		

US-CL-CURRENT: 713/165; 713/153

ABSTRACT:

A solution to the general problem of Secure Storage and Retrieval of Information (SSRI) guarantees that also the process of storing the information is correct even when some processors fail. A user interacts with the storage system by depositing a file and receiving a proof that the deposit was correctly executed. The user interacts with a single distinguished processor called the gateway. The mechanism enables storage in the presence of both inactive and maliciously active faults, while maintaining (asymptotical) space optimailty. This mechanism is enhanced with the added requirement of confidentiality of information; i.e., that a collusion of processors should not be able to learn anything about the information. Also, in this case space optimality is preserved.

31 Claims, 9 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 9

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☑ 12. Document ID: US 5991414 A

L6: Entry 12 of 13 File: USPT Nov 23, 1999

US-PAT-NO: 5991414
DOCUMENT-IDENTIFIER: US 5991414 A

TITLE: Method and apparatus for the secure distributed storage and retrieval of information

DATE-ISSUED: November 23, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Garay; Juan Alberto	Yonkers	NY		
Gennaro; Rosario	New York	NY		
Jutla; Charanjit Singh	Elmsford	NY		
Rabin; Tal D.	Riverdale	NY		

US-CL-CURRENT: 713/165; 380/30, 707/202, 709/201, 713/168, 713/180, 713/181, 713/193

ABSTRACT:

A solution to the general problem of Secure Storage and Retrieval of Information (SSRI) guarantees that also the process of storing the information is correct even when some processors fail. A user interacts with the storage system by depositing a file and receiving a proof that the deposit was correctly executed. The user interacts with a single distinguished processor called the gateway. The mechanism enables storage in the presence of both inactive and maliciously active faults, while maintaining (asymptotical) space optimailty. This mechanism is enhanced with the added requirement of confidentiality of information; i.e., that a collusion of processors should not be able to learn anything about the information. Also, in this case space optimality is preserved.

14 Claims, 9 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 9

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☑ 13. Document ID: US 5933498 A

L6: Entry 13 of 13 File: USPT Aug 3, 1999

US-PAT-NO: 5933498
DOCUMENT-IDENTIFIER: US 5933498 A

TITLE: System for controlling access and distribution of digital property

DATE-ISSUED: August 3, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Schneck; Paul B.	Potomac	MD		
Abrams; Marshall D.	Silver Spring	MD		

US-CL-CURRENT: 705/54

ABSTRACT:

A method and device are provided for controlling access to data. Portions of the data are protected and rules concerning access rights to the data are determined. Access to the protected portions of the data is prevented, other than in a non-useable form; and users are provided access to the data only in accordance with the rules as enforced by a mechanism protected by tamper detection. A method is also provided for distributing data for subsequent controlled use of those data. The method includes protecting portions of the data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing a package including: the protected portions of the data and the protected rules. A user is provided controlled access to the distributed data only in accordance with the rules as enforced by a mechanism protected by tamper protection. A device is provided for controlling access to data having protected data portions and rules concerning access rights to the data. The device includes means for storing the rules; and means for accessing the protected data portions only in accordance with the rules, whereby user access to the protected data portions is permitted only if the rules indicate that the user is allowed to access the portions of the data.

88 Claims, 35 Drawing figures
Exemplary Claim Number: 49
Number of Drawing Sheets: 26

Terms	Documents
L5 AND hash	13

Terms used **smartcard hash optimization** Found **5,124** of **151,219**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 Using smartcards to secure a personalized gambling device

William A. Aiello, Aviel D. Rubin, Martin J. Strauss

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available: pdf(762.94 KB) Additional Information: full citation, abstract, references, index terms

We introduce a technique for using an untrusted device, such as a hand-held personal digital assistant or a laptop to perform real financial transactions without a network. We utilize the tamper-resistant nature of smartcards to store value on them and perform probabilistic computations based on user input. We discuss an application of this to gambling. The technique has the properties that the user is guaranteed to make money when he wins and the house is guaranteed to make money w ...

2 PicoDBMS: Scaling down database techniques for the smartcard

Philippe Pucheral, Luc Bouganim, Patrick Valduriez, Christophe Bobineau

September 2001 **The VLDB Journal — The International Journal on Very Large Data Bases**, Volume 10 Issue 2-3

Full text available: pdf(259.03 KB) Additional Information: full citation, abstract, index terms

Smartcards are the most secure portable computing device today. They have been used successfully in applications involving money, and proprietary and personal data (such as banking, healthcare, insurance, etc.). As smartcards get more powerful (with 32-bit CPU and more than 1 MB of stable memory in the next versions) and become multi-application, the need for database management arises. However, smartcards have severe hardware limitations (very slow write, very little RAM, constrained stable mem ...

Keywords: Atomicity, Durability, Execution model, PicoDBMS, Query optimization, Smartcard applications, Storage model

3 A new public key cryptosystem based on higher residues

David Naccache, Jacques Stern

November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**

Full text available: pdf(1.00 MB) Additional Information: full citation, references, citings, index terms

4 Reliability and security: Java cryptography on KVM and its performance and security optimization using HW/SW co-design techniques

Yusuke Matsuoka, Patrick Schaumont, Kris Tiri, Ingrid Verbauwhede

September 2004 **Proceedings of the 2004 international conference on Compilers, architecture, and synthesis for embedded systems**

Full text available: pdf(188.08 KB) Additional Information: full citation, abstract, references, index terms

This paper describes a design approach to include and optimize Java based cryptographic applications into resource limited embedded devices.For easy prototyping and to be platform independent, the security applications are first developed in Java. Two Java cryptographic libraries, the Bouncy Castle API and the IAIK API are ported to a real embedded device for cost and performance evaluation. It requires 0.88Mbytes to 1.2Mbytes in the KVM footprint size and a few milliseconds to run secret key al ...

Keywords: cryptography, design, embedded systems, java, security

5 Security in embedded systems: Design challenges

Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3

Full text available: pdf(3.67 MB) Additional Information: full citation, abstract, references, index terms

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

6 DB-IR-1 (databases and information retrieval): indexing and query processing effiency: Energy management schemes for memory-resident database systems

Jayaprakash Pisharath, Alok Choudhary, Mahmut Kandemir

November 2004 **Proceedings of the Thirteenth ACM conference on Information and knowledge management**

Full text available: pdf(251.47 KB) Additional Information: full citation, abstract, references, index terms

With the tremendous growth of system memories, memory-resident databases are increasingly becoming important in various domains. Newer memories provide a structured way of storing data in multiple chips, with each chip having a bank of memory modules. Current memory-resident databases are yet to take full advantage of the banked storage system, which offers a lot of room for performance and energy optimizations. In this paper, we identify the implications of a banked memory environment in sup ...

Keywords: DRAM, database, energy, hardware energy scheme, multiquery optimization, power consumption, query-directed energy management

7 Authentication and authorization: Silicon physical random functions

Blaise Gassend, Dwaine Clarke, Marten van Dijk, Srinivas Devadas

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**

Full text available: pdf(433.69 KB) Additional Information: full citation, abstract, references, citings, index terms

We introduce the notion of a Physical Random Function (PUF). We argue that a complex integrated circuit can be viewed as a silicon PUF and describe a technique to identify and authenticate individual integrated circuits (ICs).We describe several possible circuit realizations of different PUFs. These circuits have been implemented in commodity Field Programmable Gate Arrays (FPGAs). We present experiments which indicate that reliable authentication of individual FPGAs can be performed even in the ...

Keywords: identification, physical random function, physical security, smartcard, tamper resistance, unclonability

8 Scheduling and resource allocation: Samsara: honor among thieves in peer-to-peer storage

Landon P. Cox, Brian D. Noble

October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

Full text available: pdf(290.28 KB) Additional Information: full citation, abstract, references, citings, index terms

Peer-to-peer storage systems assume that their users consume resources in proportion to their contribution. Unfortunately, users are unlikely to do this without some enforcement mechanism. Prior solutions to this problem require centralized infrastructure, constraints on data placement, or ongoing administrative costs. All of these run counter to the design philosophy of peer-to-peer systems.*Samsara* enforces fairness in peer-to-peer storage systems without requiring trusted third parties, ...

Keywords: distributed accounting, peer-to-peer storage systems

9 A survey of peer-to-peer content distribution technologies

Stephanos Androutsellis-Theotokis, Diomidis Spinellis

December 2004 **ACM Computing Surveys (CSUR)**, Volume 36 Issue 4

Full text available: pdf(517.77 KB) Additional Information: full citation, abstract, references, index terms

Distributed computer architectures labeled "peer-to-peer" are designed for the sharing of computer resources (content, storage, CPU cycles) by direct exchange, rather than requiring the intermediation or support of a centralized server or authority. Peer-to-peer architectures are characterized by their ability to adapt to failures and accommodate transient populations of nodes while maintaining acceptable connectivity and performance.Content distribution is an important peer-to-peer application ...

Keywords: Content distribution, DHT, DOLR, grid computing, p2p, peer-to-peer

10 Special session on security on SoC: Securing wireless data: system architecture challenges

Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally

October 2002 **Proceedings of the 15th international symposium on System Synthesis**

Full text available: pdf(172.35 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of current and future wireless data applications and services. This paper highlights the challenges posed by the need for security during system architecture design for wireless handsets, and provides an overview of emerging techniques

to address them. We focus on the computational requirements for securing wireless data transactions, revealing a gap between these requirements and the trends in processing capabilities of embedded processors used in wireless h ...

Keywords: 3DES, AES, DES, IPSec, RSA, SSL, WTLS, decryption, design methodology, embedded system, encryption, handset, mobile computing, performance, platform, security, security processing, system architecture, wireless communications

11 Processor microarchitecture II: AEGIS: architecture for tamper-evident and tamper-resistant processing

G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas Devadas

June 2003 **Proceedings of the 17th annual international conference on Supercomputing**

Full text available: pdf(286.90 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe the architecture for a single-chip aegis processor which can be used to build computing systems secure against both physical and software attacks. Our architecture assumes that all components external to the processor, such as memory, are untrusted. We show two different implementations. In the first case, the core functionality of the operating system is trusted and implemented in a security kernel. We also describe a variant implementation assuming an untrusted operating s ...

Keywords: certified execution, secure processors, software licensing

12 Security: HIDE: an infrastructure for efficiently protecting information leakage on the address bus

Xiaotong Zhuang, Tao Zhang, Santosh Pande

October 2004 **Proceedings of the 11th international conference on Architectural support for programming languages and operating systems**

Full text available: pdf(216.31 KB) Additional Information: full citation, abstract, references, citings, index terms

XOM-based secure processor has recently been introduced as a mechanism to provide copy and tamper resistant execution. XOM provides support for encryption/decryption and integrity checking. However, neither XOM nor any other current approach adequately addresses the problem of information leakage via the address bus. This paper shows that without address bus protection, the XOM model is severely crippled. Two realistic attacks are shown and experiments show that 70% of the code might be cracked ...

Keywords: address bus leakage protection, secure processor

13 On the fly signatures based on factoring

Guillaume Poupard, Jacques Stern

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available: pdf(786.71 KB) Additional Information: full citation, abstract, references, index terms

In response to the current need for fast, secure and cheap public-key cryptography largely induced by the fast development of electronic commerce, we propose a new on the fly signature scheme, i.e. a scheme that requires very small on-line work for the signer It combines provable security based on the factorization problem, short public and secret keys, short transmission and minimal on-line computation. It is the first RSA-like signature scheme that can be used for both ef ...

14 Just fast keying: Key agreement in a hostile internet

William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, Omer Reingold

May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2

Full text available: pdf(324.39 KB) Additional Information: full citation, abstract, references, index terms

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use in the IP security architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of tradeoffs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: Cryptography, denial-of-service attacks

15 Work-in-progress session on innovative topics: Security wrappers and power analysis for SoC technologies

C. H. Gebotys, Y. Zhang

October 2003 **Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis**

Full text available: pdf(790.57 KB) Additional Information: full citation, abstract, references, index terms

Future wireless internet enabled devices will be increasingly powerful supporting many more applications including one of the most crucial, security. Although SoCs offer more resistance to bus probing attacks, power/EM attacks on cores and network snooping attacks by malicious code are relevant. This paper presents a methodology for security on NoC at both the network level (or transport layer) and at the core level (or application layer) is proposed. For the first time a low cost security wrapp ...

Keywords: VLIW, adiabatic, design, performance, security

16 Key management and key exchange: Efficient, DoS-resistant, secure key exchange for internet protocols

William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, Angelos D. Keromytis

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**

Full text available: pdf(118.52 KB) Additional Information: full citation, abstract, references, index terms

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of trade-offs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: cryptography, denial of service attacks

17 Approaches to fault-tolerant and transactional mobile agent execution---an algorithmic view

Stefan Pleisch, André Schiper

September 2004 **ACM Computing Surveys (CSUR)**, Volume 36 Issue 3

Full text available: pdf(946.94 KB) Additional Information: full citation, abstract, references, index terms

Over the past years, mobile agent technology has attracted considerable attention, and a significant body of literature has been published. To further develop mobile agent technology, reliability mechanisms such as fault tolerance and transaction support are required. This article aims at structuring the field of fault-tolerant and transactional mobile agent execution and thus at guiding the reader to understand the basic strengths and weaknesses of existing approaches. It starts with a discu ...

Keywords: ACID, Byzantine failures, agreement problem, asynchronous system, commit, crash failures, fault tolerance, malicious places, mobile agents, replication, security, transaction

18 Logical and physical design issues for smart card databases

Cristiana Bolchini, Fabio Salice, Fabio A. Schreiber, Letizia Tanca

July 2003 **ACM Transactions on Information Systems (TOIS)**, Volume 21 Issue 3

Full text available: pdf(1.12 MB) Additional Information: full citation, abstract, references, citings, index terms

The design of very small databases for smart cards and for portable embedded systems is deeply constrained by the peculiar features of the physical medium. We propose a joint approach to the logical and physical database design phases and evaluate several data structures with respect to the performance, power consumption, and endurance parameters of read/program operations on the Flash-EEPROM storage medium.

Keywords: Design methodology, access methods, data structures, flash memory, personal information systems, smart card

19 Access control policy implementation: Succinct specifications of portable document access policies

Marina Bykova, Mikhail Atallah

June 2004 **Proceedings of the ninth ACM symposium on Access control models and technologies**

Full text available: pdf(210.88 KB) Additional Information: full citation, abstract, references, index terms

When customers need to each be given portable access rights to subset of documents from large universe of *n* vailable documents, it is often the case that the space vailable for representing each customer's access rights is limited to much less than *n*, say it is no more than *m* bits. This is the case when, e.g., limited-capacity inexpensive cards are used to store the access rights to huge multimedia document databases. How does one represent subsets of huge set of *n* el ...

Keywords: access control, access control enforcement, algorithm design, compact policy representation, computational complexity, portable access rights

20 Optimizing equijoin queries in distributed databases where relations are hash partitioned

Dennis Shasha, Tsong-Li Wang

May 1991 **ACM Transactions on Database Systems (TODS)**, Volume 16 Issue 2

Full text available: pdf(1.84 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Consider the class of distributed database systems consisting of a set of nodes connected by a high bandwidth network. Each node consists of a processor, a random access memory, and a slower but much larger memory such as a disk. There is no shared memory among the nodes. The data are horizontally partitioned often using a hash function. Such a

description characterizes many parallel or distributed database systems that have recently been proposed, both commercial and academic. We study the ...

Keywords: NP-complete problems, equijoin, hashing, relational data models, spanning trees, systems

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

PORTAL
US Patent & Trademark Office

Subscribe (Full Service) Register (Free, Limited Service) Login

Search: The ACM Digital Library The Guide

rousseau ludovic SEARCH

THE ACM DIGITAL LIBRARY

Full text of every article ever published by ACM.

- **Using the ACM Digital Library**
  - Frequently Asked Questions (FAQ's)

Recently loaded issues and proceedings:
(available in the DL within the past 2 weeks)

ACM Transactions on Applied Perception (TAP)
Volume 2 Issue 1

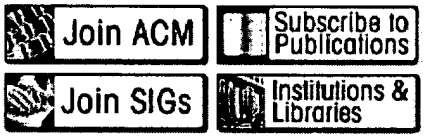
ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP)
Volume 1 Issue 1

Ubiquity
Volume 6 Issue 2

interactions
Volume 12 Issue 2

Feedback

- Report a problem
- Take our Satisfaction survey



- **Advanced Search**
- **Browse the Digital Library:**
  - Journals
  - Magazines
  - Transactions
  - Proceedings
  - Newsletters
  - Publications by Affiliated Organizations
  - Special Interest Groups (SIGs)

Personalized Services: Login required

My Binders

Save search results and queries. Share binders with colleagues and build bibliographies.

TOC Service

Receive the table of contents via email as new issues or proceedings become available.

CrossRef Search
Pilot program to create full-text interpublisher searchability.

Computing Reviews

Access critical reviews of computing literature.

THE GUIDE TO COMPUTING LITERATURE

Bibliographic collection from major publishers in computing.
Go to The Guide

Inventor name
searched all 3

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 9 of 9 returned.

☐ 1. Document ID: US 6810518 B1

L2: Entry 1 of 9 File: USPT Oct 26, 2004

US-PAT-NO: 6810518
DOCUMENT-IDENTIFIER: US 6810518 B1

TITLE: Migration of different source languages to an execution medium

DATE-ISSUED: October 26, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Grimaud; Gilles	Lille			FR
Vandewalle; Jean-Jacques	Marseille			FR

US-CL-CURRENT: 717/146; 717/139, 717/147

ABSTRACT:

The invention automatically executes, in a single execution medium, a number of programs written in source languages to which respective execution media are dedicated, without constraining a programmer to a single source language for a respective execution medium type. Each program is compiled into a program expressed in an intermediate language representing a minimum subset of the source languages. In a data processing means such as a smart card, an execution medium is dedicated to the intermediate language. The intermediate language program is loaded with a respective programming library adapting the respective source language to the intermediate language in order to execute the intermediate language program in the execution medium.

16 Claims, 11 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 8

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. D

☑ 2. Document ID: US 6754886 B1

L2: Entry 2 of 9 File: USPT Jun 22, 2004

US-PAT-NO: 6754886
DOCUMENT-IDENTIFIER: US 6754886 B1

TITLE: Method and system for storing java objects in devices having a reduced support of high-level programming concepts

DATE-ISSUED: June 22, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Merk; Lothar	Weil i.Schoenbuch			DE
Stober; Thomas	Boeblingen			DE

US-CL-CURRENT: 717/116; 710/68, 710/74, 717/103, 717/175

ABSTRACT:

The objects to be stored on a SmartCard or on a similar device are output from the host application computer in a form adapted to the device, particularly in form of a byte array which can easily be stored on such a SmartCard. That serialization comprises to convert any particular object into a sequence of bytes representing the object and its current status by storing all attributes, the name of them and all further objects which are referenced by the object which is subject to that serialization step. With the total of that information that object can be recovered in an unchanged form after any reset or interruptions which can possibly take place during usage of the SmartCard in a respective SmartCard terminal. The recover procedure is performed in analogous form: the object as well as all further objects being referenced by that object is instantiated and is initialized with the data read out from the SmartCard. The byte array representing that object can be stored both on common file system oriented SmartCards and on JavaCards, too, without being confronted to any specific further problem.

14 Claims, 3 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 3

☐ 3. Document ID: US 6687898 B2

L2: Entry 3 of 9 File: USPT Feb 3, 2004

US-PAT-NO: 6687898
DOCUMENT-IDENTIFIER: US 6687898 B2

TITLE: Optimization of n-base typed arithmetic expressions

DATE-ISSUED: February 3, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chen; Zhiqun	Palo Alto	CA		
Schwabe; Judith E.	Palo Alto	CA		

US-CL-CURRENT: 717/153; 708/498, 708/551, 708/553, 717/151

ABSTRACT:

A method for arithmetic expression optimization includes receiving a first instruction defined for a first processor having a first base, the first instruction including an operator and at least one operand, converting the first instruction to a second instruction optimized for a second processor having a second base when all operands do not carry potential overflow or when the operator is insensitive to overflow, the second base being smaller than the first base, and converting to a wider base a third instruction that is the source of the overflow when the at least one operand the potential for overflow and when the operator is sensitive to overflow. An apparatus for arithmetic expression optimization includes at least one memory having program instructions and at least one processor configured to use the program instructions to receive a first instruction defined for a first processor having a first base, convert the first instruction to a second instruction optimized for a second processor having a second base when every one of the at least one operand does not carry potential overflow or when the operator is insensitive to overflow, the second base being smaller than the first base, and convert to a wider base a third instruction that is the source of the overflow when the at least one operand the potential for overflow and when the operator is sensitive to overflow.

42 Claims, 31 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 23

☐ 4. Document ID: US 6684391 B1

L2: Entry 4 of 9 File: USPT Jan 27, 2004

US-PAT-NO: 6684391
DOCUMENT-IDENTIFIER: US 6684391 B1

TITLE: Method for operating a computer system, byte code verifier and computer system

DATE-ISSUED: January 27, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Stroetmann; Karl	Munich			DE

US-CL-CURRENT: 717/148; 717/143

ABSTRACT:

The invention is directed to a method for operating a computer system, as well as to a byte code verifier and to a computer system. The inventive method checks whether a computer program loaded onto a computer system exercises an illegal access to a variable, i.e. whether the variable is initialized before it is read. This test ensues before the execution of the program, so that such a test no longer need be performed upon execution of the program. The inventive method requires little memory space in the testing of the program and nonetheless carries out a

complete test. Since the testing ensues before the execution of the program, the program execution itself is considerably speeded up since no further test is thereby required.

11 Claims, 5 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 4

☐ 5. Document ID: US 6651186 B1

L2: Entry 5 of 9 File: USPT Nov 18, 2003

US-PAT-NO: 6651186
DOCUMENT-IDENTIFIER: US 6651186 B1
**** See image for Certificate of Correction ****

TITLE: Remote incremental program verification using API definitions

DATE-ISSUED: November 18, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Schwabe; Judith E.	Palo Alto	CA		

US-CL-CURRENT: 714/38; 717/135

ABSTRACT:

A method of operating a computer system includes providing a program in memory, verifying the program prior to an installation of the program and generating a program fault signal when the verification fails. The program includes at least one program unit, and each program unit includes an Application Programming Interface (API) definition file and an implementation. Each API definition file defines items in its associated program unit that are made accessible to one or more other program units and each implementation includes executable code corresponding to the API definition file. The executable code includes type specific instructions and data. Verification includes determining whether a first program unit implementation is internally consistent, determining whether the first program unit implementation is consistent with a first program unit API definition file associated with the first program unit implementation and generating a program fault signal when the verifying fails. A resource-constrained device includes a memory for providing a remotely verified application software program that includes at least one program unit, each program unit comprising type specific instructions and data. The resource-constrained device also includes a virtual machine that is capable of executing instructions included within the application software program. The remote verification uses an API definition file for each implementation to determine whether a first program unit implementation is internally consistent and to determine whether the first program unit implementation is consistent with a first program unit API definition file associated with the first program unit implementation.

27 Claims, 34 Drawing figures

Exemplary Claim Number: 1
Number of Drawing Sheets: 31

☐ 6. Document ID: US 6615166 B1

L2: Entry 6 of 9 File: USPT Sep 2, 2003

US-PAT-NO: 6615166
DOCUMENT-IDENTIFIER: US 6615166 B1

TITLE: Prioritizing components of a network framework required for implementation of technology

DATE-ISSUED: September 2, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Guheen; Michael F.	Tiburon	CA		
Mitchell; James D.	Manhattan Beach	CA		
Barrese; James J.	San Jose	CA		

US-CL-CURRENT: 703/27; 703/26, 709/220, 709/223, 709/231, 717/140, 719/316

ABSTRACT:

A system and method are provided for prioritizing components of an existing network framework. First, a plurality of components required for implementation of a predetermined technology using an existing network framework are provided. Next, a priority listing of the components is complied such that the relative position of the components on the priority listing corresponds to a temporal priority among the components. The existing network framework and the components are pictorially represented. Next, a first component of the existing network framework is indicia coded in order to indicate that the first component must be installed first based on the component's position on the priority listing. Thereafter, a second component and any remaining components of the existing network framework is indicia encoded in order to indicate that the second component and any remaining components must be installed after the first component based on the second component's position on the priority listing.

18 Claims, 177 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 177

☐ 7. Document ID: US 6581206 B2

L2: Entry 7 of 9 File: USPT Jun 17, 2003

US-PAT-NO: 6581206
DOCUMENT-IDENTIFIER: US 6581206 B2

TITLE: Computer program language subset validation

DATE-ISSUED: June 17, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chen; Zhiqun	Palo Alto	CA		

US-CL-CURRENT: 717/143; 717/142, 717/148

ABSTRACT:

Language subset validation includes validating multiple program modules that comprise a program. The program modules include multiple bytecodes defined for a first computer language that is a hardware-dependent subset of a second computer language. The validation includes indicating an error condition for items in the multiple program modules that are not defined for the first computer language, indicating an error condition for items in the multiple program modules that are not supported by an execution environment of the first computer language and indicating an error condition for items in the multiple program modules that are defined for the first computer language but used in a manner inconsistent with the first computer language.

60 Claims, 17 Drawing figures
Exemplary Claim Number: 55
Number of Drawing Sheets: 15

☐ 8. Document ID: US 6536037 B1

L2: Entry 8 of 9 File: USPT Mar 18, 2003

US-PAT-NO: 6536037
DOCUMENT-IDENTIFIER: US 6536037 B1
**** See image for Certificate of Correction ****

TITLE: Identification of redundancies and omissions among components of a web based architecture

DATE-ISSUED: March 18, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Guheen; Michael F	Tiburon	CA		
Mitchell; James D.	Manhattan Beach	CA		
Barrese; James J.	San Jose	CA		

US-CL-CURRENT: 717/151; 703/2, 709/231

ABSTRACT:

A system, method and article of manufacture are provided for conveying redundancies and omissions among components of a network framework such as a web architecture framework. First, an area of an existing network framework is determined in which redundancies and omissions exist. Next, a pictorial representation of the existing network framework is presented along with a plurality of its components. The foregoing redundancies and the omissions are then highlighted by indicia coding the components of the existing network that reside in the area. As such, a diagnostic analysis of redundant efforts and gaps in a current implementation of the existing network framework is effectively conveyed.

19 Claims, 177 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 177

☐ 9. Document ID: US 6308317 B1

L2: Entry 9 of 9 File: USPT Oct 23, 2001

US-PAT-NO: 6308317
DOCUMENT-IDENTIFIER: US 6308317 B1

TITLE: Using a high level programming language with a microcontroller

DATE-ISSUED: October 23, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Wilkinson; Timothy J.	London			GB
Guthery; Scott B.	Belmont	MA		
Krishna; Ksheerabdhi	Cedar Park	TX		
Montgomery; Michael A.	Cedar Park	TX		

US-CL-CURRENT: 717/139; 717/141, 717/146

ABSTRACT:

An integrated circuit card is used with a terminal. The integrated circuit card includes a memory that stores an interpreter and an application that has a high level programming language format. A processor of the card is configured to use the interpreter to interpret the application for execution and to use a communicator of the card to communicate with the terminal.

87 Claims, 25 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 23

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L1 AND 717/$$$.ccls.	9

Display Format: REV Change Format

Previous Page Next Page Go to Doc#

Google Web Images Groups News Froogle Local[New!] more »
sun microsystems java card optimization Search Advanced Search Preferences

Web Results **1 - 10** of about **25,000** for **sun microsystems java card optimization**. (**1.17** seconds)

Java **Card** Technology for Smart **Cards**: Architecture and ...
... ubiquitous Java platform for smart **cards** and other ... that designed and implemented Java **Card** APIs and is currently working on **Sun's** Java **Card** virtual machine ...
java.sun.com/docs/books/**javacard**/ - 13k - Cached - Similar pages

Java **Card** Technology for Smart **Cards**: Architecture and ...
... independent, ubiquitous Java platform for smart **cards** and other ... a staff engineer in the Java **Card** engineering team at **Sun Microsystems**, Inc., developed ...
java.sun.com/developer/Books/consumerproducts/**javacard**/ - 14k - Cached - Similar pages
[More results from java.sun.com]

CastleCops - Java **Card** Update Shows Full Hand of IT Issues
... Java **Card** 2.2.1 specification, **Sun Microsystems** Inc ... The new Java **Card** specification also continues the trend ... My conversation with **Sun's** Peter Cattaneo concluded ...
castlecops.com/article4194.html - Similar pages

banner
... JavaBeans (EJ, Jakarta ORO, **Optimization**, Uneditable Atomic ... Foundation Profile, Java **Card**, Pascal, Modula-2, Oberon, XML ... are trademarks of **Sun Microsystems**, Inc. ...
www.esus.com/docs/Alpha.jsp - 48k - Cached - Similar pages

INédit 17 - Researcher's speaking - Java **Card** - a programming ...
... It was designed by **Sun Microsystems**, in collaboration with the ... to prove the security of a Java **Card** application. ... http://www.irisa.fr/lande/jensen/**javacard**.html. ...
www.inria.fr/actualites/inedit/inedit17_rega.en.html - 6k - Cached - Similar pages

J2ME : MicroDevNet : Tools
... Mobile Information Device Profile (MIDP), **Sun Microsystems**, Inc. ... of Java **Card** SIM Toolkit applications (Java **Card** applets running on GSM SIM **cards**). ...
www.micro**java**.com/developer/tools - 46k - Cached - Similar pages

[PDF] SecurJC Platform 0177-1
File Format: PDF/Adobe Acrobat - View as HTML
... vendors that supply 32-bit smart **cards** equipped with ... The Java **Card** VM and GlobalPlatform Loader have been written ... Java is a trademark of **Sun Microsystems**, Inc. ...
www.arm.com/pdfs/177-1%20SecurJC%20Platform.pdf - Similar pages

sun Java
... names, Web hosts, HTML, **optimization**, promotion, and ... **Sun** Microsystem's new Java **Card** enterprise software enhances ... As part of **Sun Microsystems'** extensive online ...
www.firstwebsitedesign.com/ Traffic%20equalizer%20pre27th%20Dec%2004/14/web-design1569.html - 9k - Cached - Similar pages

Sun IT Learning Link
... experience in learning Java, **Sun Microsystems**, in collaboration with ... units deployed worldwide, Java **Card** technology is ... Administrator The **Sun** Certified Security ...
www.sesfocus.com/issue29/issueth29.html - 23k - Cached - Similar pages

Sun IT Learning Link
... can be deployed on a single **card**, and new ... language can be executed securely on **cards** from different ... THE NETWORK IS THE COMPUTER © 2004 **Sun Microsystems**, Inc. ...
www.sesfocus.com/issue29/issueau29.html - 20k - Cached - Similar pages
[More results from www.sesfocus.com]

Goooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

sun microsystems java card optimiz Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google